Patent Claims

1. A method for authorizing a transaction by a user using a terminal (18) which is capable of communicating with a background system (10), with steps performed by the terminal (18):
   - determining (30) identification information (32) which identifies the user,
   - sending (34) data (36) to the background system (10) to authenticate the terminal (18) at the background system (10) and to transmit user identification data (ID) from which the identity of the user can be derived, to the background system (10),
   - receiving secret data (SEC) assigned to the user from the background system (10),
   - playing back (48) a secret (50) given by the secret data (SEC) to the user,
   - determining (58) a personal feature (56) of the user, and
   - sending (60) data (62) which is related to the personal feature (56) of the user to the background system (10) to signal or document the authorization of the transaction by the user.

2. The method according to Claim 1, characterized in that the terminal (18) sends to the background system (10) a message secured with a MAC or a cryptographic signature for authentication at the background system (10).

3. The method according to Claim 2, characterized in that the message contains the user identification data (ID) that corresponds to the

identification information (32) determined by the terminal (18) or has been derived from it.

4. The method according to any one of Claims 1 through 3, characterized in that the secret (50) played back to the user is a text and/or acoustic and/or visual and/or tactile information.

5. The method according to any one of Claims 1 through 4, characterized in that transaction data (54) is also displayed to the user.

6. The method according to any one of Claims 1 through 5, characterized in that the personal feature (56) is a biometric feature of the user.

7. The method according to any one of Claims 1 through 6, further characterized by the step of receiving acknowledgement data (CD) from the background system (10) and displaying and/or printing out an acknowledgement (78) for the user.

8. A method for authorizing a transaction by a user, the method using a background system (10) capable of communicating with a terminal (18), with steps performed by the background system (10):

- receiving data (36) from the terminal (18), the data (36) authenticating (38) the terminal (18) at the background system (10), the identity of the user being derivable from the data (36),
- if the authentication (38) of the terminal (18) at the background system (10) has been successful, then accessing (40) secret data (SEC) stored in a database (14) and assigned to the user, and sending (42) data (44) from which the secret data (SEC) can be determined, to the terminal (18), and

- receiving data (62) from the terminal (18), the data (62) pertaining at least to a personal feature (56) of the user and documenting the authorization of the transaction by the user.

9. The method according to Claim 8, characterized in that the secret data (SEC) pertains to a secret (50) which changes from one transaction to the next.

10. The method according to Claim 9, characterized in that the secret data (SEC) pertains to a secret (50) which depends at least in part on transactions performed previously.

11. The method according to any one of Claims 8 through 10, characterized in that the data (62) which pertains at least to the personal feature (56) of the user is checked (66), and the transaction is considered as authorized by the user only if this check is successful.

12. The method according to Claim 11, characterized in that acknowledgement data (CD) is sent to the terminal (18) if the check is successful.

13. A method for authorizing a transaction by a user using a terminal (18) capable of communicating with a background system (10), with the steps:

- determining (30), by the terminal (18), identification information (32) which identifies the user,
- communicating between the terminal (18) and the background system (10) to authenticate (38) the terminal (18) at the background system (10) and to transmit user identification data

(ID) from which the identity of the user can be derived to the background system (10),

- if the authentication (38) of the terminal (18) at the background system (10) has been successful, then the background system (10) accesses secret data (SEC) stored in a database (14) and assigned to the user, and data (44) from which the secret data (SEC) can be determined is sent (42) to the terminal (18),
- playing back (48), by the terminal (18), a secret (50) given by the secret data (SEC) to the user,
- determining (58), by the terminal (18), a personal feature (56) of the user, and
- performing the transaction using data (62) pertaining at least to the personal feature (56) of the user.

14. The method according to Claim 13, characterized in that the communication processes between the terminal (18) and the background system (10) are protected from attacks at least in part by time stamps (TS1-TS4) and/or sequence numbers and/or random numbers and/or an encryption with a session key.

15. The method according to Claim 13 or Claim 14, further characterized by method steps performed by the terminal (18) according to any one of Claims 1 through 7 and/or method steps performed by the background system (10) according to any one of Claims 8 through 12.

16. A device, in particular a terminal (18) and/or a background system (10), equipped for executing a method according to any one of Claims 1 through 15.

17. A computer program product having program instructions for at least one processor of a terminal (18) and/or a background system (10) to cause the at least one processor to execute a method according to any one of Claims 1 through 15.